Rapport Technique :

Projet d'
Administration Systèmes et Réseaux

Groupe 11 :

Manuelle Ndamtang

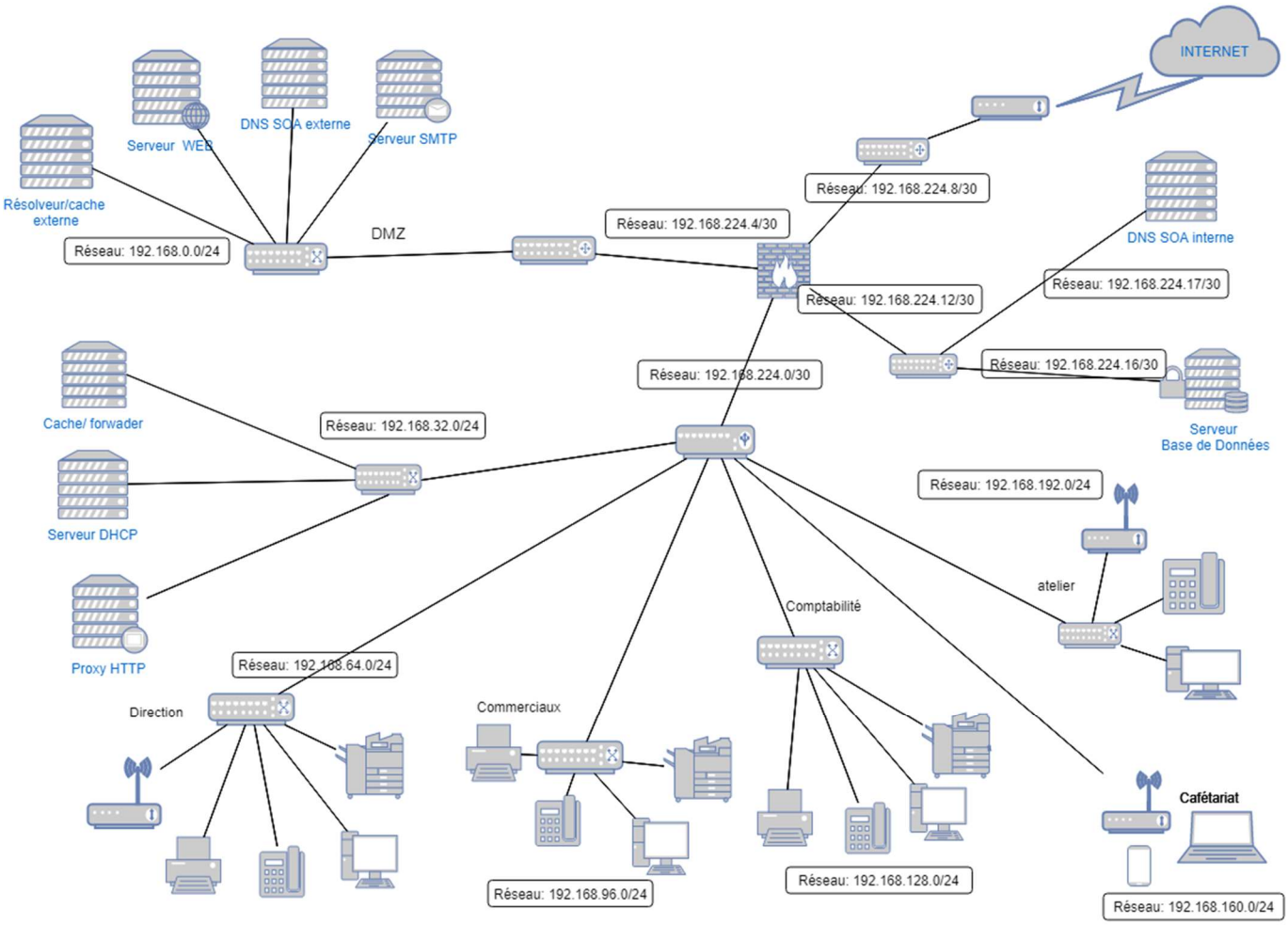
Darryl Bilongo

Supervisé par :

Virgine Van Den Schrieck

14 Mars 2019

1 Schéma physique



Legende


Photocopieuse


telephone


PC


Access-point


switch


Laptop


routeur


Serveur


Switch Layer 3

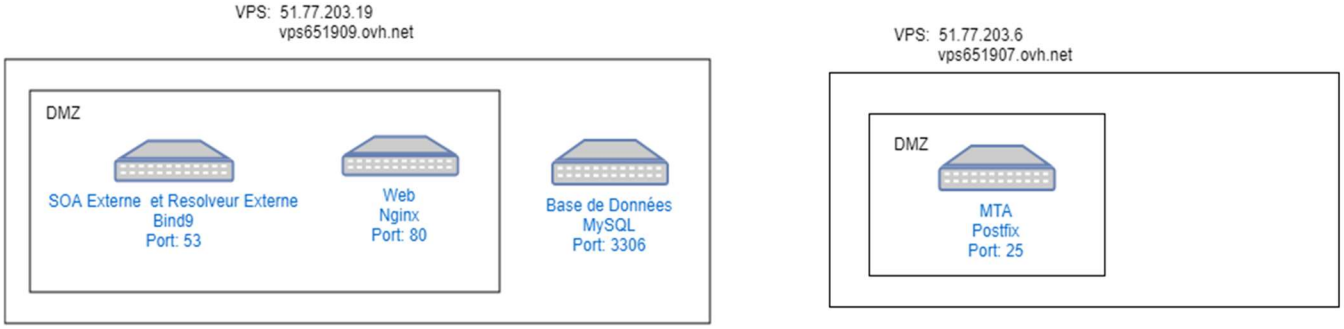

modem


GSM


firewall


imprimante

2 Schéma Prototype



3 Explications des choix d'agencement des Schémas

3.1 Schéma physique

- Pour ce qui concerne la DMZ, sachant que celui-ci doit être un sous réseau isolé séparant le réseau local et internet via le firewall, notre DMZ héberge les machines du réseau qui ont besoin d'être directement accessible depuis l'extérieur. C'est pourquoi se trouve le serveur web, le serveur SOA externe…
- Pour concevoir cette architecture, nous avons utilisé un seul pare-feu avec quatre interfaces. A la première interface, le firewall est connecté au réseau externe formé du firewall et du FAI. La deuxième délimitant, pour des questions de sécurité le serveur base de données et le reste de réseaux ainsi que le SOA interne :
  Le serveur base de données parce qu'il contient des données plus ou moins confidentielles de l'entreprise et qu'il est important de l'isoler tout en s'assurant que des services lui faisant appel sont autorisés. Le SOA interne fournissant la structure ainsi les différents services internes à l'entreprise.
  La troisième interface connecté au LAN, et le dernier à la DMZ.
- Le souci au niveau de cette architecture est le suivant :
  si cet unique firewall est compromis (par un pirate par exemple) toute cette architecture est aussi compromise. Nous y réfléchirons sur des moyens plutôt sûrs pour y remédier.

4 Service DNS

4.1 Difficultés Rencontrés :

La difficulté à mettre en place le DNS était lié aux manques de connaissances des différents outils de débogage. En plus de cela, une erreur qui empêchait le service DNS de fonctionner en dehors du container était l'ACL mis en place pour la résolution externe.

4.2 Maintenance

Sur ce plan, nous avons opté pour une configuration des journaux systèmes. Prenant en compte le fait que les fichiers logs peuvent donc être très volumineux, on a défini le nombre de version du fichier pouvant être mémorisé de deux à trois versions. Ensuite on mit en place une répartition des fichiers logs en fonction des catégories des requêtes. Ainsi nous avons les fichiers logs pour les requêtes client, pour les atteintes à la sécurité et le service bind9.

5 Service Web

Pour le service Web, nous avons rencontré des difficultés sur la mise en place du serveur Nginx. En effet au départ, la compréhension de Docker fut un frein considérable dans l'avancement de la configuration. La recherche de l'information était compliquée et beaucoup de tutoriels était souvent sans aboutissement concrets.

Nous avons tout de même réussi à mettre en place le serveur et à vérifier l'affichage des différents sites. Cependant, les fonctionnalités essentielles pour le fonctionnement de notre serveur en cohérence avec les spécificités de la solution tel que le contenu dynamique en PHP et la sécurisation des sites en HTTPS n'ont pas pu être finalisés. Nous sommes tout de même en bon chemin pour les réaliser dans les prochains jours.

6 Service mail

La configuration du serveur SMTP est toujours en cours de réalisation. Nous avons utilisé Postfix pour mettre la configuration du notre MTA. Il fonctionne bien en interne comme en externe, sauf de les emails arrivés à destination, se retrouvent dans le Spam du récepteur.

6.1 Difficultés

Une des principales difficultés dans la configuration du service mail était la configuration du fichier « resolv.conf » du containeur docker. Le principal but de cette configuration était de spécifier le serveur DNS ainsi que le domaine auquel appartient le serveur mail. Ce qui ne fut pas facile car l'opération consistant à copier un fichier de la machine hôte vers l'image tout en s'assurant d'avoir modifié les permissions était sans issus.

Après des nombreuses recherches, nous avons compris que le seul moyen d'apporter les modifications sur ce fichier du containeur était au niveau des options du démarrage du container.

Coté sécurité nous avons encore du chemin à faire. La configuration du DKIM a été faite. Maintenant il ne reste plus qu'a configurer le SPF et le DMARC.

7 Serveur DB

Nous avons mis en place un serveur de base de données MySQL en créant une base de données de départ et un utilisateur admin. Pour l'instant les mots de passes sont en clair pour besoin de test mais nous travaillons pour le sécuriser avec SSL.